UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

NETAPP, INC., Plaintiff, v. NIMBLE STORAGE, INC., MICHAEL REYNOLDS, an individual, DANIEL WEBER, an individual, SANDHYA KLUTE, an individual, TIMOTHY BINNING, an individual, NEIL GLICK, an individual, CHRISTOPHER ALDUINO, an individual, and Does 1-50, Defendants.	Case No.: 5:13-CV-05058-LHK (HRL) ORDER GRANTING IN PART AND DENYING IN PART DEFENDANTS' MOTIONS TO DISMISS

Plaintiff NetApp, Inc. filed this suit against Defendants Nimble Storage, Inc. ("Nimble"), Michael Reynolds, and former NetApp employees Daniel Weber, Sandhya Klute, Timothy Binning, Neil Glick, and Christopher Alduino (collectively, "employees"). *See* ECF Nos. 1 (Compl.), 34 (First Am. Compl.). Nimble, Reynolds, and the group of employees have each moved to dismiss all claims against them on multiple grounds. *See* ECF Nos. 40, 41, 42. NetApp has opposed all motions and requested jurisdictional discovery in connection with Reynolds. The Court held a hearing on the motions on May 8, 2014. The Court addresses all four motions together. Having considered the briefing, the oral arguments, the record in this case, and

applicable law, the Court GRANTS IN PART AND DENIES IN PART the motions for the reasons stated below.

I. BACKGROUND

A. NetApp's Lawsuit

NetApp and Nimble are competing companies in the data storage industry. First Am. Compl. ¶ 31. Defendants Weber, Klute, Binning, Glick, and Alduino are former NetApp employees who now work for Nimble. *Id.* ¶¶ 7-11. Defendant Reynolds is an Australian citizen and resident who works at Nimble Storage Australia Pty Limited, an entity related to Defendant Nimble (discussed below). *Id.* ¶ 6. This lawsuit stems from NetApp's belief that "Nimble targeted NetApp talent and proprietary and confidential information to compete unfairly in the marketplace." *Id.* ¶ 36. NetApp alleges that "Nimble has achieved rapid growth and customer adoption" by "rely[ing] heavily on foundational information as to the internal working of NetApp's products and its proprietary business processes." *Id.* ¶ 31.

According to NetApp, Reynolds previously worked at Thomas Duryea Consulting ("TDC"), an "IT infrastructure consultancy business" in Australia. *Id.* ¶ 39. NetApp contracted with TDC for certain services, provided Reynolds with access to NetApp's computer systems, and offered Reynolds training courses available to NetApp employees, all subject to NetApp's restrictions on unauthorized access and use of its systems. *See id.* ¶¶ 41-46. Reynolds left TDC in April 2013 and took a job with Nimble where—NetApp alleges—he accessed NetApp databases repeatedly from June through August 2013 and used confidential, proprietary information to solicit business for Nimble. *See id.* ¶¶ 47-54.

Regarding its former employees sued here, NetApp claims that each person worked at NetApp until early- to mid-2013, before departing the company for Nimble. NetApp accuses each former employee of breaching a common "Proprietary Information and Inventions Agreement" by taking, copying, or destroying volumes of confidential NetApp data before leaving. *See, e.g., id.* ¶¶ 62 (alleging that Weber took "sales material; pricing models; sales strategies; and detailed customer information"), 80 (alleging that "two days before his departure from NetApp, Glick took

steps to delete and/or render unrecoverable, inaccessible, and/or unavailable NetApp Company Documents and Materials stored on his NetApp computer.").

B. Procedural History

On October 29, 2013, NetApp filed this lawsuit, alleging a variety of claims against Nimble and individual defendants Reynolds, Weber, Klute, and other unnamed "Doe" defendants, based on alleged unauthorized access to NetApp's computer systems and theft of proprietary information.[1] Compl. ¶¶ 59-123. On December 20, 2013, the named Defendants collectively filed three motions to dismiss, arguing that NetApp failed to plead sufficient facts to support various claims and challenging subject matter jurisdiction, supplemental jurisdiction, and personal jurisdiction as to Reynolds. *See* ECF Nos. 22-24.

On December 23, 2013, NetApp filed a motion for leave to conduct jurisdictional discovery in connection with Reynolds's challenge to personal jurisdiction, along with a motion to expedite a hearing on its motion for leave. *See* ECF Nos. 26, 25. On January 6, 2014, Nimble and Reynolds each filed an opposition to NetApp's motion for jurisdictional discovery. *See* ECF Nos. 29, 30. On January 13, 2014, NetApp filed a reply in support of its discovery motion. *See* ECF No. 36. On January 7, 2014, Court denied NetApp's motion to expedite. *See* Order, ECF No. 33. On January 17, 2014, the Court entered an order by stipulation in which NetApp agreed to withdraw its motion for jurisdictional discovery without prejudice, subject to renewal after amending its complaint. *See* Order, ECF No. 39. The parties have since renewed their dispute over jurisdictional discovery. *See* Discovery Dispute Joint Report #1, ECF No. 43; Order, ECF No. 64.

On January 10, 2014, NetApp filed a First Amended Complaint, adding individual defendants Binning, Glick, and Alduino. *See* First Am. Compl. ¶¶ 74-82. NetApp pleaded claims against the various defendants for violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030, "CFAA"), trespass to chattel, trade secret misappropriation, breach of contract, intentional interference with contract and contractual relations, and unfair competition. *See id.* ¶¶ 83-176.

[1] NetApp has filed at least two other suits related to alleged misconduct by former employees. *NetApp, Inc. v. Baker*, No. CIV524121 (Cal. Super. Ct.), *NetApp, Inc. v. Walsh*, No. 1:13cv1176 (E.D. Va.).

On February 18, 2014, Defendants filed new motions to dismiss all claims in the First Amended Complaint, again challenging the sufficiency of NetApp's pleadings as to various claims and jurisdictional issues. Nimble sought to dismiss NetApp's state law claims due to lack of supplemental jurisdiction, and moved to dismiss all claims for failure to state a claim or—in the alternative—for a more definite statement under Rule 12(e). *See* ECF No. 40 ("Nimble Mot."). Reynolds moved to dismiss for lack of personal jurisdiction and for failure to state any claim against him, and further sought to join and incorporate by reference the motions filed by Nimble and the individual Defendants. *See* ECF No. 41 ("Reynolds Mot."). All of the former employee Defendants (Weber, Klute, Binning, Glick, and Alduino) collectively moved to dismiss for lack of supplemental jurisdiction and failure to state any claims, and also sought to join and incorporate by reference the motions filed by Nimble and Reynolds. *See* ECF No. 42 ("Employees Mot.").

On March 27, 2014, NetApp filed an opposition to each motion to dismiss, along with supporting declarations and a request for judicial notice of certain facts related to Nimble's operations. *See* ECF Nos. 45 ("NetApp Reynolds Opp'n"), 50 ("NetApp Employees Opp'n"), 51 ("NetApp Nimble Opp'n"), 49 (NetApp Request for Judicial Notice). On April 10, 2014, all Defendants filed replies. *See* ECF Nos. 58 ("Nimble Reply"), 59 ("Employees Reply"), 60 ("Reynolds Reply"). The Court held a hearing on May 8, 2014.

II. LEGAL STANDARDS

A. Motion to Dismiss Under Rule 12(b)(6)

A complaint must contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). If a plaintiff fails to plead "enough facts to state a claim to relief that is plausible on its face," the complaint may be dismissed for failure to state a claim upon which relief may be granted. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007); Fed. R. Civ. P. 12(b)(6). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). "The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (internal quotation marks omitted). For purposes of ruling on a Rule

12(b)(6) motion, a court "accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008).

"Generally, the scope of review on a motion to dismiss for failure to state a claim is limited to the contents of the complaint." *Marder v. Lopez*, 450 F.3d 445, 448 (9th Cir. 2006). However, a court need not accept as true allegations contradicted by judicially noticeable facts, *Shwarz v. United States*, 234 F.3d 428, 435 (9th Cir. 2000), and the "[C]ourt may look beyond the plaintiff's complaint to matters of public record" without converting the Rule 12(b)(6) motion into one for summary judgment, *Shaw v. Hahn*, 56 F.3d 1128, 1129 n.1 (9th Cir. 1995). Nor is the court required to "'assume the truth of legal conclusions merely because they are cast in the form of factual allegations.'" *Fayer v. Vaughn*, 649 F.3d 1061, 1064 (9th Cir. 2011) (per curiam) (quoting *W. Mining Council v. Watt*, 643 F.2d 618, 624 (9th Cir. 1981)). Mere "conclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss." *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004); *accord Iqbal*, 556 U.S. at 678. Furthermore, "a plaintiff may plead herself out of court" if she "plead[s] facts which establish that [s]he cannot prevail on h[er] . . . claim." *Weisbuch v. Cnty. of Los Angeles*, 119 F.3d 778, 783 n.1 (9th Cir. 1997) (internal quotation marks omitted).

B. Motion to Dismiss Under Rule 12(b)(2) for Lack of Personal Jurisdiction

In a motion challenging personal jurisdiction under Rule 12(b)(2), the plaintiff, as the party seeking to invoke the jurisdiction of the federal court, has the burden of establishing that jurisdiction exists. *See Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 800 (9th Cir. 2004). When the motion to dismiss constitutes a defendant's initial response to the complaint, the plaintiff need only make a prima facie showing that personal jurisdiction exists. *See Data Disc, Inc. v. Sys. Tech. Assocs., Inc.*, 557 F.2d 1280, 1285 (9th Cir. 1977). While a plaintiff cannot "'simply rest on the bare allegations of its complaint,' uncontroverted allegations in the complaint must be taken as true [and] [c]onflicts between parties over statements contained in affidavits must be resolved in the plaintiff's favor." *Schwarzenegger*, 374 F.3d at 800 (quoting *Amba Mktg. Sys.*,

Inc. v. Jobar Int'l, Inc., 551 F.2d 784, 787 (9th Cir. 1977), and citing *AT&T v. Compagnie Bruxelles Lambert*, 94 F.3d 586, 588 (9th Cir. 1996)).

C. Supplemental Jurisdiction

While a federal court may exercise supplemental jurisdiction over state-law claims "that are so related to claims in the action within [the court's] original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution," 28 U.S.C. § 1367(a), a court may decline to exercise supplemental jurisdiction where a state claim "substantially predominates over the claim or claims over which the district court has original jurisdiction," *id.* § 1367(c)(2); *see also Albingia Versicherungs A.G. v. Schenker Int'l, Inc.*, 344 F.3d 931, 937-38 (9th Cir. 2003) (§ 1367(c) grants federal courts the discretion to dismiss state law claims when all federal claims have been dismissed). A court, in considering whether to retain supplemental jurisdiction, should consider factors such as "economy, convenience, fairness, and comity." *Acri v. Varian Assocs.*, 114 F.3d 999, 1001 (9th Cir. 1997) (en banc) (internal quotation marks omitted).

D. Leave to Amend

"Dismissal with prejudice and without leave to amend is not appropriate unless it is clear . . . that the complaint could not be saved by amendment." *Eminence Capital, LLC v. Aspeon, Inc.*, 316 F.3d 1048, 1052 (9th Cir. 2003). When dismissing a complaint for failure to state a claim, "a district court should grant leave to amend even if no request to amend the pleading was made, unless it determines that the pleading could not possibly be cured by the allegation of other facts." *Lopez v. Smith*, 203 F.3d 1122, 1130 (9th Cir. 2000) (en banc) (quoting *Doe v. United States*, 58 F.3d 494, 497 (9th Cir. 1995)). Nonetheless, a court "may exercise its discretion to deny leave to amend due to . . . 'futility of amendment.'" *Carvalho v. Equifax Info. Servs., LLC*, 629 F.3d 876, 892-93 (9th Cir. 2010) (citation omitted).

III. DISCUSSION

Defendants present numerous legal theories that potentially dispose of various causes of action on multiple, interdependent grounds. Supplemental jurisdiction over NetApp's state law claims depends in part on the viability of its CFAA claim, which is the only federal cause of action and is asserted against only Nimble and Reynolds. Both of those Defendants challenge the

sufficiency of the CFAA claims under Rule 12(b)(6), while Reynolds also challenges personal jurisdiction. The Court first addresses Reynolds's personal jurisdiction challenge, then the sufficiency of NetApp's CFAA claims, followed by supplemental jurisdiction, and the sufficiency of NetApp's remaining claims within the Court's jurisdiction.

As an initial matter, the Court addresses NetApp's Request for Judicial Notice. ECF No. 49. While a district court generally may not consider any material beyond the pleadings in ruling on a Rule 12(b)(6) motion, a court may take judicial notice of documents referenced in the complaint, as well as matters in the public record, without converting a motion to dismiss into one for summary judgment. *See Lee v. City of Los Angeles*, 250 F.3d 668, 688-89 (9th Cir. 2001). A matter may be judicially noticed if it is either "generally known within the trial court's territorial jurisdiction" or "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b). NetApp requests judicial notice of four Nimble webpages and excerpts from a Nimble filing with the Securities and Exchange Commission. Khachakourian Decl. Exs. L, O-R (ECF Nos. 45-13, -16 to -19). Defendants have not opposed, and the materials are either referenced in the First Amended Complaint or matters in the public record. Accordingly, the Court grants NetApp's Request for Judicial Notice.

A. Personal Jurisdiction Over Reynolds

An Australian resident, Reynolds contends that this Court lacks personal jurisdiction over him. Reynolds Mot. at 6-14. NetApp argues primarily that the Court has specific personal jurisdiction based on Reynolds's efforts to access NetApp's computer systems in California, with only a cursory argument regarding general jurisdiction. NetApp Reynolds Opp'n at 6-14. The Court agrees with NetApp with respect to specific jurisdiction.

Where no applicable federal statute governs personal jurisdiction, the court applies the law of the state in which it sits. *See* Fed. R. Civ. P. 4(k)(1)(A); *Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316, 1320 (9th Cir. 1998). "Because California's long-arm jurisdictional statute is coextensive with federal due process requirements, the jurisdictional analyses under state law and federal due process are the same." *Schwarzenegger*, 374 F.3d at 800-01. "For a court to exercise personal jurisdiction over a nonresident defendant, that defendant must have at least 'minimum

contacts' with the relevant forum such that the exercise of jurisdiction 'does not offend traditional notions of fair play and substantial justice.'" *Id.* at 801 (quoting *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945)).

To determine whether a defendant's contacts with the forum state are sufficient to establish specific jurisdiction, the Ninth Circuit employs a three-part test:

> (1) The non-resident defendant must purposefully direct his activities or consummate some transaction with the forum or resident thereof; or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws;
>
> (2) the claim must be one which arises out of or relates to the defendant's forum-related activities; and
>
> (3) the exercise of jurisdiction must comport with fair play and substantial justice, *i.e.* it must be reasonable.

Id. at 802 (quoting *Lake v. Lake*, 817 F.2d 1416, 1421 (9th Cir. 1987)). Plaintiff bears the burden of satisfying the first two prongs. *Sher v. Johnson*, 911 F.2d 1357, 1361 (9th Cir. 1990). If Plaintiff does so, then the burden shifts to Defendant to "set forth a 'compelling case' that the exercise of jurisdiction would not be reasonable." *CollegeSource, Inc. v. AcademyOne, Inc.*, 653 F.3d 1066, 1076 (9th Cir. 2011) (quoting *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 476-78 (1985)). The Court addresses each of the three prongs in turn.

1. Purposeful Direction and Availment

The standard under the first prong differs for claims sounding in tort and claims sounding in contract. *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 433 F.3d 1199, 1206 (9th Cir. 2006). For tort claims, the "purposeful direction" standard generally applies, and for contract claims, the "purposeful availment" test generally applies. *Id.* Here, NetApp alleges both tort and contract claims against Reynolds based on the same underlying conduct—unauthorized access to NetApp's computers (discussed below)—so both standards are relevant. *See Action Embroidery Corp. v. Atl. Embroidery, Inc.*, 368 F.3d 1174, 1180 (9th Cir. 2004) ("Personal jurisdiction must exist for each claim asserted against a defendant."). The Court determines that the first prong is satisfied as to all claims against Reynolds.

a. Purposeful Direction

To meet the "purposeful direction" standard for tort-related conduct, Reynolds's activities must satisfy a three-part "effects test" under *Calder v. Jones*, 465 U.S. 783 (1984): (1) commission of an intentional act, (2) expressly aimed at the forum state, (3) causing harm that Reynolds knew was likely to be suffered in the forum state. *Schwarzenegger*, 374 F.3d at 803. "In any personal jurisdiction case we must evaluate all of a defendant's contacts with the forum state, whether or not those contacts involve wrongful activity by the defendant." *Yahoo!*, 433 F.3d at 1207.

The first part of the effects test requires "an intent to perform an actual physical act in the real world, rather than an intent to accomplish a result or consequence of that act." *Schwarzenegger*, 374 F.3d at 806. Here, NetApp alleges that Reynolds "intentionally" accessed computer systems and obtained secure information without permission. First Am. Compl. ¶¶ 16, 85, 87, 88. Additionally, NetApp submitted supporting declarations with exhibits. *See* ECF Nos. 46-48 (Bruce, Davied, and Sun Declarations). Those materials include records documenting Reynolds's access to NetApp's computers and notices shown to users of those computers, further indicating that Reynolds purposefully accessed systems in California after receiving notice of where those systems were located. *E.g.*, ECF Nos. 47-3 (list of access dates for Reynolds), 48-2 (screenshot of Synergy Data Privacy Policy). These facts and allegations are sufficient to satisfy this part of the test because they demonstrate intentional activities.

The second part of the effects test turns on whether Reynolds "expressly aimed" his intentional acts at California. "The 'express aiming' analysis depends, to a significant degree, on the specific type of tort at issue." *Schwarzenegger*, 374 F.3d at 807. As explained above, all of Reynolds's alleged transgressions (under all pleaded causes of actions) involve improper access to NetApp's computer systems in California. NetApp claims that Reynolds received password-protected access to its computer systems as part of his work for TDC (First Am. Compl. ¶¶ 41, 44); that the NetApp systems and databases at issue were located in California at all relevant times; (*id.* ¶¶ 41, 45); that Reynolds received multiple notices that NetApp and the computer systems were located in California (*id.* ¶¶ 16, 45, 51); that Reynolds repeatedly accessed multiple NetApp systems between June and August 2013 after leaving TDC (*id.* ¶ 49); and that Reynolds accepted a

EULA (end user license agreement) that restricted access to certain databases, was deemed executed in California, and is governed by California law (*id.* ¶ 51). *See also* Venkatesan Decl. (ECF No. 41-2) ¶ 3, Ex. A (purported NetApp EULA submitted by Reynolds; "This EULA shall be deemed to have been made in . . . the State of California.").

Reynolds disputes the adequacy of these allegations, pointing out that all of his relevant acts occurred in Australia while employed with Australian companies, and that he never knew that the systems he accessed were in California. *See* Reynolds Mot. at 10-12; Reynolds Reply at 5-8. Reynolds also submits a declaration in which he maintains: "Throughout my employment at TDC and to this day, I do not know, and have never known, where the information on these databases is located." Reynolds Decl. (ECF No. 22-1) ¶ 10. However, these arguments do not defeat jurisdiction in this case. Based on NetApp's factual allegations, Reynolds had, at minimum, reason to know that he was accessing NetApp's computer systems in California. Moreover, courts have held that similar activities over the Internet can be sufficient to support personal jurisdiction. In *Panavision*, the Ninth Circuit affirmed personal jurisdiction over an individual defendant who allegedly registered as Internet domain names trademarks of a company with a principal place of business in California. 141 F.3d at 1321. The court rejected the defendant's argument that "he has not directed any activity toward Panavision in California" because "the injury occurred in cyberspace," holding that such activities satisfied the "effects test." *Id.* at 1322. More recently, this district found personal jurisdiction over out-of-state parties who accessed the Facebook website because they specifically directed actions towards the website, even if those parties did not know Facebook's physical location: "Here, there is no dispute that PNS and Williams were fully aware that Facebook existed, and that they specifically targeted their conduct against Facebook. That they were able to do so while remaining ignorant of Facebook's precise location may render this case factually distinct from prior precedents finding jurisdiction for acts of express aiming, but not in a manner that warrants a different result." *Facebook, Inc. v. ConnectU LLC*, No. C 07-01389, 2007 WL 2326090, at *6 (N.D. Cal. Aug. 13, 2007).

Reynolds's counter-examples are distinguishable. Reynolds cites *Jewish Defense Organization, Inc. v. Superior Court of Los Angeles County*, in which a California court ruled that

"defendants' conduct in registering Rambam's name as a domain name and posting passive Web sites on the Internet is not sufficient to subject them to jurisdiction in California." 72 Cal. App. 4th 1045, 1060 (1999). However, the court distinguished *Panavision* because there was no basis to conclude that the company's principal place of business was in California, and noted specifically that the defendant's activities were "passive." *Id.* at 1059, 1060 n.4. By contrast, Reynolds's alleged violations did not involve "passive" activities or merely visiting a foreign website, but rather deliberately accessing NetApp's proprietary databases to take information after performing work for NetApp and receiving repeated notices of access restrictions. As another example, Reynolds relies on *Pfister v. Selling Source, LLC*, where the District of Nevada rejected the argument that running a "highly interactive website" would support personal jurisdiction, noting that "courts within this circuit have rejected the contention that server location within the forum can constitute a basis for the exercise of personal jurisdiction." 931 F. Supp. 2d 1109, 1116 (D. Nev. 2013). However, that case specifically addressed *general* jurisdiction and noted that the location of a server did not support "*continuous and systematic* contacts." *Id.* (emphasis added). Thus, *Pfister* does not foreclose specific jurisdiction based on Reynolds's alleged conduct here. The Court finds sufficient allegations that Reynolds "expressly aimed" activities at California.

The third part of the effects test examines whether Reynolds's acts caused harm that Reynolds knew would likely occur in California. NetApp has alleged that Reynolds harmed NetApp by taking and disseminating confidential information. *See* First Am. Compl. ¶¶ 52-53. Reynolds does not deny that he knew that NetApp was located in California, and as explained above, if Reynolds did in fact repeatedly misappropriate sensitive information from NetApp's computers, he would have known that he was injuring NetApp. Accordingly, this part of the effects test is met.

b. Purposeful Availment

All three parts of the effects test are satisfied, which demonstrates "purposeful direction" as to the tort-based claims. As to the contract-based claims, the parties dispute whether Reynolds's acceptance and breach of the Synergy EULA (*e.g.*, First Am. Compl. ¶¶ 51, 115) suffices to demonstrate "purposeful availment." *See* Reynolds Mot. at 9-10. The Court need not resolve this

dispute because "a court may assert pendent personal jurisdiction over a defendant with respect to a claim for which there is no independent basis of personal jurisdiction so long as it arises out of a common nucleus of operative facts with a claim in the same suit over which the court does have personal jurisdiction." *Action Embroidery*, 368 F.3d at 1180-81 (adopting doctrine of pendent personal jurisdiction); *see also Wash. Shoe Co. v. A-Z Sporting Goods Inc.*, 704 F.3d 668, 673 (9th Cir. 2012) (following *Action Embroidery*). Here, both the contract-based claims and the tort-based claims are based on common factual predicates: Reynolds's unauthorized computer access.[2] Therefore, under Ninth Circuit precedent, specific jurisdiction over the contract claims is appropriate in this circumstance.

2. Forum-Related Activities

Under the second prong of the Ninth Circuit's analysis for specific jurisdiction, the court must determine whether NetApp's claims arise from or are related to Reynolds's forum-related activities. This inquiry turns on whether NetApp "would not have been injured 'but for'" Reynolds's alleged misconduct. *Panavision*, 141 F.3d at 1322. Here, there can be no dispute that Reynolds's activities towards California relate directly to NetApp's causes of action, which are all based on his unauthorized access to NetApp's computers.

3. Reasonableness

Under the third prong, Reynolds bears the burden of presenting a "compelling case" that jurisdiction here would not comport with "fair play and substantial justice," based on seven established factors: "(1) the extent of the defendants' purposeful injection into the forum state's affairs; (2) the burden on the defendant of defending in the forum; (3) the extent of the conflict with the sovereignty of the defendant's state; (4) the forum state's interest in adjudicating the dispute; (5) the most efficient judicial resolution of the controversy; (6) the importance of the forum to the plaintiff's interest in convenient and effective relief; and (7) the existence of an alternative forum." *CollegeSource*, 653 F.3d at 1079. Here, Reynolds argues that subjecting him to jurisdiction in California would be burdensome because he lives in Australia and has otherwise

[2] As explained below, the Court exercises supplemental jurisdiction over the state law claims against Reynolds because they form a common nucleus of operative facts with the CFAA claim.

minimal contacts with the state. *See* Reynolds Mot. at 13-14. While the Supreme Court has counseled that foreign defendants may face "unique burdens," *Asahi Metal Indus. Co. v. Superior Court of Cal.*, 480 U.S. 102, 114 (1987), courts have appropriately exercised jurisdiction over foreign parties, *e.g.*, *Yahoo!*, 433 F.3d at 1211 (personal jurisdiction over French defendants). *See also Ajuba Int'l, L.L.C. v. Saharia*, 871 F. Supp. 2d 671, 683-84 (E.D. Mich. 2012) (personal jurisdiction over Indian defendant for trade secret misappropriation claims). Additionally, California's interest in adjudicating any harm that occurred here favors jurisdiction, and Reynolds has not shown that any alternative forum exists.

Reynolds also contends that "NetApp's assertion impermissibly broadens personal jurisdiction, as any person in the world receiving materials from a California corporation could be haled into California court." Reynolds Mot. at 11. This concern is misleading. As explained above, Reynolds is not accused of passively "receiving materials" or simply setting up a website, but rather intentionally accessing a former client's databases for financial gain. NetApp points out that the legislative history of the CFAA suggests that Congress intended to address foreign activity. *See* S. Rep. No. 104-357 (1996) (noting that prior version of CFAA omitted "computers used in foreign communications or commerce, despite the fact that hackers are often foreign-based"). Reynolds has not demonstrated that it would be unreasonable for this Court to assert jurisdiction over a person who purposefully intrudes on a secure computer system in California.

Accordingly, the Court denies Reynolds's motion to dismiss for lack of personal jurisdiction. NetApp's motion for leave to conduct jurisdictional discovery is denied as moot in light of the Court's ruling on personal jurisdiction and the case schedule set at the May 8, 2014 Case Management Conference (ECF No. 65).

B. CFAA Claims

The Court next addresses the sufficiency of NetApp's claims under Rule 12(b)(6). NetApp's only cause of action based on federal law is its CFAA claim against Nimble and Reynolds. Because supplemental jurisdiction over all other claims depends on the sufficiency of NetApp's federal claims, the Court addresses the CFAA claims first.

The CFAA imposes civil liability on whoever:

> intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer (18 U.S.C. § 1030(a)(2)(C));
>
> knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $ 5,000 in any 1-year period (*id.* § 1030(a)(4));
>
> (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss (*id.* § 1030(a)(5)).

NetApp alleges that Nimble violated § 1030(a)(2)(C) vicariously by having Reynolds, as its agent, intentionally and impermissibly access NetApp's computers and obtain secret information; that Reynolds and Nimble violated § 1030(a)(4) by intending to defraud NetApp; and that Reynolds and Nimble violated all subsections of § 1030(a)(5) by damaging NetApp's computer systems. First Am. Compl. ¶¶ 85-88. NetApp also contends that Nimble and Reynolds conspired to violate the CFAA. *Id.* ¶ 84; *see also* § 1030(b) ("Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.").

The Defendants raise several challenges to the sufficiency of NetApp's CFAA claims under Rule 12(b)(6), which the Court addresses in turn.

1. "Without Authorization or Exceeding Authorized Access"

First, Reynolds argues that NetApp failed to plead facts that could support an inference that he accessed any computers "without authorization" or by "exceeding authorized access," which is required by all asserted CFAA provisions (§§ 1030(a)(2)(C), (a)(4), and (a)(5)). *See* Reynolds Mot. at 14-17. Reynolds argues that his access to NetApp's systems was never revoked, even after he stopped working for TDC, and therefore he did not breach any "technological barriers," which Reynolds claims is a requirement to demonstrate lack of authorization under the CFAA. *See* Reynolds Reply at 9. In response, NetApp contends that CFAA liability does not require circumvention of any technological barriers, and that Reynolds lost his permission to access

NetApp's systems (and knew that he lost that permission) as soon as he left TDC and no longer performed services for NetApp. *See* NetApp Reynolds Opp'n at 15-19.

This Court agrees with NetApp that the scope of authorized computer access for purposes of the CFAA does not depend entirely on circumvention of a technological barrier. The Ninth Circuit and the Northern District of California have not squarely resolved whether computer access is unauthorized or exceeds authorization under the CFAA when a person has authorization under an employment arrangement, but then changes jobs, and the computer's owner has not disabled that person's access through technological controls. However, the weight of current authority supports NetApp's interpretation.

In *LVRC Holdings LLC v. Brekka*, the Ninth Circuit confronted a similar case where a company accused a former employee of violating the CFAA by e-mailing himself sensitive documents while employed and by continuing to access the company's private website after his employment ended. 581 F.3d 1127 (9th Cir. 2009). The court first addressed the definitions of "without authorization" and "exceeds authorized access," concluding that "without authorization" in the CFAA refers only to access without any permissions at all: "we hold that a person uses a computer 'without authorization' under §§ 1030(a)(2) and (4) when the person has not received permission to use the computer *for any purpose* (such as when a hacker accesses someone's computer without any permission), or *when the employer has rescinded permission to access the computer and the defendant uses the computer anyway*." *Id.* at 1135 (emphases added). By contrast, the court observed that "[t]he definition of the term 'exceeds authorized access' from § 1030(e)(6) implies that an employee can violate employer-placed limits on accessing information stored on the computer and still have authorization to access that computer." *Id.* Accordingly, the *Brekka* court held that "an individual who is authorized to use a computer for certain purposes but goes beyond those limitations is considered by the CFAA as someone who has 'exceed[ed] authorized access.' On the other hand, a person who uses a computer 'without authorization' has no rights, limited or otherwise, to access the computer in question." *Id.* at 1133.

Based on these definitions, *Brekka* affirmed summary judgment that the worker's access while employed could not violate the CFAA because "there is no dispute that Brekka had

permission to access the computer." *Id.* at 1133, 1135. As to post-employment access, the Ninth Circuit also affirmed summary judgment of no CFAA liability due to insufficient evidence that any such access occurred, but noted: "There is no dispute that if Brekka accessed LVRC's information on the LOAD website *after he left the company* in September 2003, Brekka would have accessed a protected computer 'without authorization' for purposes of the CFAA." *Id.* at 1136 (emphasis added). This indicates that the parties and the court recognized that post-employment access could be "without authorization," even in the absence of a technological barrier.

After *Brekka*, the Ninth Circuit further addressed the scope of "authorization" under the CFAA in its en banc decision in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012). *Nosal* also involved a former employee, charged under the criminal provisions of the CFAA for violating § 1030(a)(4) by asking current employees to steal confidential information to help him start a competing business. *Id.* at 856. Relying on the text and legislative history of the CFAA and *Brekka*, the Ninth Circuit rejected the views of other Circuit Courts of Appeals and held that "the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions." *Id.* at 863. Therefore, as an example, a person who has permission to access customer lists for use in preparing invoices does not "exceed authorized access" if she impermissibly gives those customer lists to a competitor. The court reasoned that a contrary interpretation would vastly expand liability for everyday electronic activities, and "millions of unsuspecting individuals would find that they are engaging in criminal conduct." *Id.* at 859. Accordingly, the court dismissed the CFAA charge because "Nosal's accomplices had permission to access the company database and obtain the information contained within." *Id.* at 864.

In exploring the contours of "exceeds authorized access," the *Nosal* court interpreted this phrase narrowly because the CFAA is "a statute whose general purpose is to punish hacking—*the circumvention of technological access barriers*—not misappropriation of trade secrets—a subject Congress has dealt with elsewhere." *Id.* at 863 (emphasis added). At the same time, the court characterized "exceeds authorized access" to "refer to someone who's authorized to access only certain data or files but accesses unauthorized data or files—what is colloquially known as 'hacking.' For example, assume an employee is permitted to access only product information on

the company's computer but accesses customer data: He would 'exceed[ ] authorized access' if he looks at the customer lists." *Id.* at 856-57. Based on the foregoing statements, *Nosal* stated that the CFAA targets circumvention of "technological barriers" and "hacking," but also suggested that accessing information that an employee does not have permission to access at all could fall within the CFAA. Moreover, *Nosal* did not directly address a situation like Reynolds'—although Nosal was a former employee, the accomplices who allegedly stole information were current employees with authorized access. Thus, the Ninth Circuit's current interpretation of the CFAA does not foreclose liability in Reynolds' situation.

Furthermore, subsequent cases interpreting *Brekka* and *Nosal* indicate that a non-technological barrier can revoke authorization. In *Weingand v. Harland Financial Solutions, Inc.*, another court in this district held that access by a former employee whose credentials still functioned could support a CFAA claim. No. C-11-3109 EMC, 2012 U.S. Dist. LEXIS 84844 (N.D. Cal. June 19, 2012). There, the defendant company sought leave to plead a CFAA counterclaim alleging that its former employee accessed 2,700 files without authorization "after his employment with Harland as a Senior Field Engineer was terminated." *Id.* at *2. The court rejected the employee's contention that the counterclaim would not survive a motion to dismiss, concluding: "Previous Ninth Circuit authority (un-altered by *Nosal*) indicates that if a former employee accesses information without permission, *even if his prior log-in information is still operative as a technical matter*, such access would violate the CFAA." *Id.* at *9 (emphasis added) (citing *Brekka*, 581 F.3d at 1136). The court further explained:

> Although Plaintiff's counsel contended at oral argument that Plaintiff's level of verbal (or non-technical) authorization was irrelevant because the only "authorization" to which the statute speaks is "code" authorization (*i.e.*, whether someone is literally blocked from certain files by some security measure such as a password), Plaintiff offers no authority to support such a narrow interpretation. It is true that *Nosal* uses the phrase "physical access" to describe the expansive interpretation of the CFAA the government proposed (and the court rejected). *Nosal*, 676 F.3d at 857 (rejecting the government's proposition that "the language could refer to someone who has unrestricted physical access to a computer, but is limited in the use to which he can put the information"). However, the previous sentence of the opinion makes clear that the court was concerned only with the distinction between access and use, not with any distinction between types of authorization pertaining to access.

Id. at *7-9. Thus, *Weingand* expressly rejects Reynolds' theory about the scope of authorized access under the CFAA. *See also Hat World, Inc. v. Kelly*, No. CIV. S-12-01591, 2012 U.S. Dist. LEXIS 113060, at *14-15 (E.D. Cal. Aug. 10, 2012) (as to CFAA claim that former employee "accessed those computers after he resigned," "the court concludes that plaintiff has stated a claim under the CFAA by alleging facts from which the court can plausibly conclude that defendant exceeded his authorized access by continuing to access information stored on company computers and servers after his resignation").

Reynolds does not distinguish *Weingand*, but rather points out that he "was never employed by NetApp" and "was authorized to access NetApp's databases at the time of the alleged conduct." Reynolds Reply at 10. However, neither of those points forecloses liability under the CFAA. NetApp alleges that Reynolds lost authorization when he stopped working for TDC, and also knew that NetApp's databases were restricted to "NetApp employees and registered NetApp partners." First Am. Compl. ¶¶ 47, 51.

Reynolds relies on several other CFAA cases, but those are distinguishable. For example, Reynolds cites *Enki Corp. v. Freedman*, No. 5:13-cv-02201-PSG, 2014 U.S. Dist. LEXIS 9169 (N.D. Cal. Jan. 23, 2014), to argue that an employee who has access to an employer's computers cannot act without authorization. *See* Reynolds Mot. at 14-15. However, *Enki* dismissed CFAA claims where, unlike Reynolds, the alleged unauthorized access occurred *during* employment: "*Before this termination*, however, Freedman and Zuora accessed the Nimsoft servers on Zuora's network without authorization." *Enki*, 2014 U.S. Dist. LEXIS 9169 at *3 (emphasis added). *See also Integral Dev. Corp. v. Tolat*, No. C 12-06575 JSW, 2013 U.S. Dist. LEXIS 153705, at *11 (N.D. Cal. Oct. 25, 2013) (dismissing CFAA claims; "at the time of the alleged acquisition of the materials, Tolat was working for Integral"). Other courts dismissing CFAA claims have done so when unauthorized access occurred prior to termination. *E.g.*, *Quad Knopf, Inc. v. S. Valley Bio. Consulting*, No. 1:13-CV-01262, 2014 U.S. Dist. LEXIS 46985, at *11 (E.D. Cal. Apr. 3, 2014) (dismissing CFAA claims where employees were "employed at the time of the alleged transmittal"). Reynolds' reliance on *Synopsys, Inc. v. Atoptech, Inc.*, No. C 13-2965 SC, 2013 U.S. Dist. LEXIS 153089 (N.D. Cal. Oct. 24, 2013), is also misplaced. *See* Reynolds Mot. at 16.

Synopsys did not hold that the CFAA requires breach of a technical barrier; rather, it observed that "[n]either the Ninth Circuit nor Congress has fully explored the limits of this nuanced distinction," and that "an alleged breach must be pled with enough clarity and plausibility to state that access itself—not just a particular use—was prohibited." 2013 U.S. Dist. LEXIS 153089 at *32-34.

Nimble notes that this district has held that the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502, requires breach of a technological barrier, and argues that the same limitation should apply to the CFAA. *See* Nimble Mot. at 17-18. Nimble is correct that in *Facebook, Inc. v. Power Ventures, Inc.*, the court held that § 502 is limited to "use and access that circumvents technical or code-based barriers." No. C 08-05780, 2010 U.S. Dist. LEXIS 93517, at *35 (N.D. Cal. July 20, 2010); *see also In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 716 (N.D. Cal. 2011) ("However, Plaintiffs do not allege that Defendant circumvented technical barriers to gain access to a computer, computer network or website."). However, § 502 is an entirely different statute than the CFAA, and Nimble identifies no authorities holding that the two laws must be co-extensive with respect to unauthorized access. *See, e.g.*, *Enki*, 2014 U.S. Dist. LEXIS 9169 at *9-10 (analyzing CFAA and § 502 separately).

NetApp analogizes this case to a conventional property crime, arguing that "[u]nder Reynolds' theory, a thief has license to burglarize a house because a window is left open." NetApp Reynolds Opp'n at 15. However, a closer analogy would be a situation where a houseguest receives a key, is then told he is no longer welcome but keeps the key, and the homeowner neglects to change the lock. Reynolds's arguments suggest that if the former houseguest continues to re-enter the house, the houseguest would not be acting "without authorization" or "exceed[ing] authorized access," even though he knows he may not return. Current CFAA doctrine does not allow this result. Accordingly, Reynolds's arguments do not warrant dismissal of any of NetApp's CFAA claims on this basis.

2. Fraud Pleading Standard

For all asserted CFAA provisions (§§ 1030(a)(2)(C), (a)(4), and (a)(5)), Nimble and Reynolds[3] argue that CFAA claims require pleading with particularity because they resemble fraud allegations, which have specific pleading standards under Fed. R. Civ. P. 9(b), and that NetApp failed to set forth sufficient specificity. Nimble Mot. at 20. Defendants rely primarily on *Oracle America, Inc. v. Service Key, LLC*, where another court in this district held that Rule 9(b)'s heightened pleading requirements applied to the CFAA allegations at issue there. No. C 12-00790 SBA, 2012 WL 6019580, at *6 (N.D. Cal. Dec. 3, 2012). However, the weight of authority counsels that Rule 9(b) does not constrain NetApp's CFAA claims here.

First, NetApp correctly points out that, at minimum, Nimble fails to parse CFAA § 1030(a)(4) from §§ 1030(a)(2)(C) and (a)(5). As noted above, § 1030(a)(4) targets persons who "knowingly and *with intent to defraud*, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct *furthers the intended fraud* and obtains anything of value" (emphases added). By contrast, §§ 1030(a)(2)(C) and (a)(5) contain no reference to "fraud." Indeed, Nimble cites a case that expressly distinguishes those provisions for pleading purposes: "Violations of subsections (a)(2) and (a)(5) do not need to be pled with particularity." *Prop. Rights Law Grp., P.C. v. Lynch*, No. 13-00273, 2013 WL 4791485, at *4 (D. Haw. Sep. 16, 2013). Thus, Nimble provides no basis for imputing a fraud pleading standard to §§ 1030(a)(2)(C) or (a)(5).

Second, most CFAA cases in this district have not applied Rule 9(b)'s pleading standards to all CFAA claims. In *eBay Inc. v. Digital Point Solutions, Inc.*, the court ruled that eBay's CFAA allegations based on violations of a user agreement were adequately pleaded, and that "'fraud' under the CFAA only requires a showing of unlawful access; there is no need to plead the elements of common law fraud to state a claim under the Act." 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009); *see also Facebook, Inc. v. Maxbounty, Inc.*, 274 F.R.D. 279, 284 (N.D. Cal. Mar. 28, 2011)

[3] Reynolds does not make this argument in his motion, but joins and incorporates by reference Nimble's motion. Reynolds Mot. at 1; *see also* Fed. R. Civ. P. 12(g). The Court does not approve of attempts to circumvent page limits, but addresses this argument as to both Defendants for completeness.

(citing *eBay*; "The Court sees no reason to depart from its previous analysis."); *Multiven v. Cisco*, 725 F. Supp. 2d 887, 892 (N.D. Cal. 2010) ("For purposes of the CFAA, '[t]he term "defraud" . . . simply means wrongdoing and does not require proof of common law fraud.'") (citation omitted); *Oracle Am., Inc. v. TERiX Computer Co.*, No. 5:13-cv-03385-PSG, 2014 U.S. Dist. LEXIS 561, at *16-17 (N.D. Cal. Jan. 3, 2014) (refusing to apply Rule 9(b) to CFAA).

Third, *Service Key* does not require a contrary result. There, the court found that "*[i]n the instant case*," the CFAA claims required heightened pleading because Oracle specifically alleged fraudulent inducement and fraudulent trafficking of passwords. 2012 WL 6019580 at *6 (emphasis added). The court also discussed *Kearns v. Ford Motor Co.*, where the Ninth Circuit held that a plaintiff must plead certain statutory claims with particularity *if* fraud is alleged: "While fraud is *not a necessary element of a claim* under the CLRA and UCL, a plaintiff may nonetheless allege that the defendant engaged in fraudulent conduct. . . . *In that event*, the claim is said to be 'grounded in fraud' or to 'sound in fraud,' and the pleading . . . as a whole must satisfy the particularity requirement of Rule 9(b)." 567 F.3d 1120, 1125 (9th Cir. 2009) (emphases added). Thus, read together, the foregoing precedents require that CFAA claims under § 1030(a)(4) be pleaded with specificity only when fraudulent conduct is specifically alleged as the basis for the wrongdoing. *See TERiX*, 2014 U.S. Dist. LEXIS 561, at *16 ("Even accepting *Service Key* as persuasive authority, the court does not conclude that Rule 9(b) applies to Oracle's CFAA allegations in this case. The reason is that Oracle's allegations here cannot be said to rely entirely on a course of conduct that is fraudulent under California law."). Here, NetApp has alleged that Reynolds and Nimble engaged in wrongdoing under the CFAA, but not any patterns of fraudulent conduct at issue in *Service Key* and *Kearns*. *E.g.*, First Am. Compl. ¶ 54. Accordingly, Rule 9(b) does not apply to NetApp's § 1030(a)(4) claims in this case.

3. "Damage"

Nimble and Reynolds argue that NetApp failed to plead any "damage" under the CFAA. Defendants raise this argument with respect to § 1030(a)(5) of the CFAA, but not §§ 1030(a)(2)(C) or (a)(4). Section 1030(a)(5) requires "damage" to a plaintiff's computer systems. Section 1030(e)(8) defines "damage" as "any impairment to the integrity or availability of data, a program,

a system, or information." However, Defendants cite multiple cases holding that "damage" means harm to computers or networks, not economic harm due to the commercial value of the data itself. *See Capitol Audio Access, Inc. v. Umemoto*, No. 2:13-cv-00134, 2013 WL 5425324, at *2-3 (E.D. Cal. Sept. 27, 2013); *New S. Equip. Mats, LLC v. Keener*, No. 3:13CV162, 2013 WL 5946371, at *6-8 (S.D. Miss. Nov. 5, 2013) (collecting cases); *Farmers Ins. Exchange v. Steele Ins. Agency, Inc.*, No. 2:13-cv-00784, 2013 WL 3872950, at *21 (E.D. Cal. July 25, 2013) ("Indeed, a number of courts have noted that 'costs not related to computer impairment or computer damages are not compensable under the CFAA.'" (citation omitted)). *See also PNC Mortg. v. Superior Mortg. Corp.*, No. 09-5084, 2012 U.S. Dist. LEXIS 25238, at *10-11 (E.D. Pa. Feb. 27, 2012) (holding that harm "in the form of lost customers, lost customer relationships and other injuries" "is not sufficient to state a claim under the CFAA"); *Andritz, Inc. v. S. Maint. Contractor, LLC*, 626 F. Supp. 2d 1264, 1266 (M.D. Ga. 2009) (holding "lost revenue caused by the misappropriation of proprietary information and intellectual property from an employer's computer" was "not recoverable under CFAA"); § 1030(e)(11) (separately defining "loss" as "any reasonable cost").

NetApp does not plead any such "damage" in plausible detail, alleging only "harm to the integrity of its data, programs, and computer system." First Am. Compl. ¶ 90. Indeed, NetApp alleges only that Reynolds accessed its databases without permission, not that he damaged any systems or destroyed any data. *See id.* ¶ 49. In its Opposition, NetApp does not distinguish the cases above, but instead points to conclusory allegations of harm under its separate claim for trespass to chattel, and claims that its databases were damaged because that information "derives value from its exclusivity." NetApp Nimble Opp'n at 12-13. Therefore, NetApp has failed to plead facts showing any cognizable damage under the CFAA. Accordingly, NetApp's CFAA claims against Reynolds and Nimble under § 1030(a)(5) are dismissed with leave to amend.

4. Allegations Specific to Nimble

NetApp alleges that Nimble violated the CFAA under two theories: (1) Nimble is vicariously liable for Reynolds's acts, and (2) Nimble conspired with Reynolds. *See* First Am. Compl. ¶¶ 84-85. NetApp claims that Nimble violated § 1030(a)(2)(C) "with Reynolds acting as

its agent in the course and scope of his employment and for the benefit of his employer Nimble," and that "Reynolds and Nimble" violated §§ 1030(a)(4) and (a)(5). *Id.* ¶¶ 85-87.

As to vicarious liability, courts have held that an employer can be vicariously liable for an employee's violations of the CFAA if those transgressions occur in the scope of employment or the employer directs the employee's conduct. *See, e.g., SBM Site Servs., LLC v. Garrett*, No. 10-cv-00385, 2012 U.S. Dist. LEXIS 24130, at *15 (D. Colo. Feb. 27, 2012) ("It is reasonable to infer that Garrett accessed SBM's laptop during the time that he was employed with Able and in the scope of such employment."); *Charles Schwab & Co. v. Carter*, No. 04 C 7071, 2005 U.S. Dist. LEXIS 21348, at *20 (N.D. Ill. 2005) ("the Court assumes that Congress drafted the CFAA with an intent to permit vicarious liability"). Here, Nimble argues that NetApp failed to plead facts that could show that Nimble directly employed or controlled Reynolds. The Court agrees. NetApp alleges that Reynolds "is a Systems Engineer with Nimble Storage Australia Pty Limited ('Nimble AUS'), the Australian proprietary company controlled by Nimble." First Am. Compl. ¶ 6. Thus, NetApp identified "Nimble" and "Nimble AUS" as separate (if related) entities. However, NetApp now tries to argue that "Reynolds was a Nimble employee," NetApp Nimble Opp'n at 6, even though NetApp repeatedly pleaded that Reynolds's employment was "with Nimble AUS," First Am. Compl. ¶¶ 48-49. *Cf. id.* ¶ 47 (referring to Reynolds "working for Nimble"). Although NetApp alleges that Nimble handles certain operations like recruitment and hiring for Nimble AUS (*id.* ¶ 48), there are no allegations that Nimble AUS was Nimble's alter ego, or that Nimble directed Reynolds's unauthorized access.[4] *See City of Los Angeles v. San Pedro Boat Works*, 635 F.3d 440, 453 (9th Cir. 2011) (noting "ordinary rule that an employee's knowledge may be imputed only to his employer, and not to the employer's parent company"). NetApp asserts that Reynolds "used" stolen information "on behalf of Nimble" (*id.* ¶ 54), but even if these vague allegations were true, they would not establish that Reynolds violated the CFAA at Nimble's behest. Accordingly, NetApp has not sufficiently pleaded vicarious liability against Nimble.

[4] NetApp cites correspondence that supposedly shows that Nimble answered queries to Nimble AUS. *See* Khachatourian Decl. ¶¶ 8-9, Exs. F, G. Those facts are outside the complaint and should not be considered in a motion to dismiss. *See Marder*, 450 F.3d at 448.

Regarding conspiracy, NetApp's First Amended Complaint also falls short. For allegations under § 1030(b), other courts have required specific allegations of an agreement and common activities to state a conspiracy claim. *See Trademotion, LLC v. Marketcliq, Inc.*, 857 F. Supp. 2d 1285, 1294 (M.D. Fla. 2012) (recommending dismissal of § 1030(b) claim due to lack of facts showing "a knowing agreement with another to commit the unlawful act"); *Vacation Club Servs., Inc. v. Rodriguez*, No. 6:10-cv-247, 2010 U.S. Dist. LEXIS 39572, at *5-6 (M.D. Fla. Apr. 22, 2010). In the context of civil conspiracy, "[t]o survive a motion to dismiss, plaintiff must allege with sufficient factual particularity that defendants reached some explicit or tacit understanding or agreement." *Alfus v. Pyramid Tech. Corp.*, 745 F. Supp. 1511, 1521 (N.D. Cal. 1990). In this case, NetApp provides no factual allegations that indicate a conspiracy other than the bare statement that "Reynolds and Nimble conspired to commit acts." First Am. Compl. ¶ 83. The Court need not assume that such legal conclusions are true. *See Iqbal*, 556 U.S. at 678.

NetApp's claims against Nimble under the CFAA are hereby dismissed with leave to amend. In seeking to amend its complaint, NetApp must address the deficiencies above.

C. Supplemental Jurisdiction

Because the parties are not completely diverse, *see* First Am. Compl. ¶¶ 5-11, NetApp's CFAA claim provides the sole basis for federal subject matter jurisdiction in this case. NetApp's remaining causes of action against Nimble and Reynolds are based on state law, and all causes of action against its former employees involve state law. A federal court may exercise supplemental jurisdiction over state law claims "that are so related to claims in the action within [the court's] original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution." 28 U.S.C. § 1367(a). Conversely, a court may decline to exercise supplemental jurisdiction where "the claim substantially predominates over the claim or claims over which the district court has original jurisdiction." *Id.* § 1367(c)(2). As noted above, a court should consider "economy, convenience, fairness, and comity." *Acri*, 114 F.3d at 1001 (internal quotation marks omitted).

1. Claims Against Former Employees

NetApp has pleaded claims for trade secret misappropriation against Klute and Weber, breach of contract against all employees, intentional interference with contract and contractual relations against Weber, and unfair competition against all employees. *See* First Am. Compl. Of the eleven enumerated causes of action, seven involve state law claims pleaded exclusively against the former employees. The employees argue that these claims do not form a common nucleus of operative facts with the CFAA claims against Nimble and Reynolds and, in the alternative, that these claims predominate over the CFAA allegations. *See* Employees Mot. at 6-8. The Court agrees that supplemental jurisdiction is not appropriate here.

First, the Court is not convinced that a common factual nucleus exists here. NetApp asserts that there is a locus for all claims against all Defendants because the state law claims involve "(1) Nimble, the employer common to all defendants; (2) interpretation of the terms of identical NetApp employment contracts, the obligations arising therefrom, to be construed under California law; and (3) relate to a common scheme executed by Nimble and by the individual defendants to harm NetApp's business interests." First Am. Compl. ¶ 22; *see also* NetApp Employees Opp'n at 7 (claiming a "wide-ranging plot"). These bare allegations of a "common scheme" fail to establish sufficient factual overlap. As explained above, NetApp's CFAA claims are based on Reynolds's unauthorized access. Reynolds was a contractor, not a NetApp employee, and his alleged misconduct occurred in Australia after he switched to Nimble AUS. Reynolds never signed a NetApp employment contract. By contrast, the former employees allegedly stole information while working for NetApp in the United States, and at least Weber and Binning allegedly discussed stealing secrets for Nimble together. *See* First Am. Compl. ¶¶ 58, 61. Thus, contrary to NetApp's contentions, interpretation of the NetApp employment contract is irrelevant for Reynolds. *See Titan Global LLC v. Rasmussen*, No. 12-CV-2104-LHK, 2012 U.S. Dist. LEXIS 171484, at *35-36 (N.D. Cal. Dec. 2, 2012) (declining supplemental jurisdiction over claim requiring interpretation of agreement not at issue in other claims). NetApp does not allege that Reynolds collaborated with—or even knew—any of the five former NetApp employees, and therefore offers no basis for finding

a "common scheme" between Reynolds and these employees who are the other individual Defendants in this case.[5]

The parties cite several cases involving supplemental jurisdiction related to causes of action that do not involve the CFAA and are not directly analogous. *E.g., Taiwan Semiconductor Mfg. Co. v. Semiconductor Mfg. Int'l Corp.*, No. C-03-5761-MMC, 2004 U.S. Dist. LEXIS 29717 (N.D. Cal. Apr. 21, 2004) (patent infringement, trade secret, and unfair competition claims against common defendants); *Monolithic Power Sys., Inc. v. O2 Micro Int'l, Ltd.*, Nos. C 04-2000, C 06-2929, 2006 WL 2839134, at *4 (N.D. Cal. Oct. 3, 2006) (patent infringement and unfair competition against common defendants). However, other courts have declined supplemental jurisdiction over state law claims despite retaining a CFAA claim. *E.g.*, *Contemporary Servs. Corp. v. Hartman*, No. 08-02967, 2008 WL 3049891, at *4 (C.D. Cal. Aug. 4, 2008) (dismissing multiple claims under § 1367(c)(2) because "Plaintiffs' state law claims involve a broader scope of issues and proof than the CFAA claim"); *Deman Data Sys., LLC v. Schessel*, No. 8:12-cv-2580-T-24, 2014 U.S. Dist. LEXIS 13063, at *17-20 (M.D. Fla. Feb. 3, 2014) (dismissing unjust enrichment claim under § 1367(a), but retaining others, despite CFAA claim). In other recent cases, courts have retained state law claims in connection with a CFAA claim, but in situations where both sets of claims were asserted against the same defendants. *E.g.*, *NovelPoster v. Javitch Canfield Grp.*, No. 13-cv-05186-WHO, 2014 U.S. Dist. LEXIS 46375, at *15-16 (N.D. Cal. Apr. 1, 2014); *Absolute Energy Solutions, LLC v. Trosclair*, No. H-13-3358, 2014 U.S. Dist. LEXIS 12772, at *10 (S.D. Tex. Feb. 3, 2014). Here, all of NetApp's claims against the employees are exclusively the province of state law and bear little factual relation to the CFAA allegations.

Second, even if the claims against the employees were sufficiently related to the CFAA claims to form a common case or controversy under § 1367(a), the Court exercises its discretion under § 1367(c)(2) to decline supplemental jurisdiction. *See United Mine Workers v. Gibbs*, 383 U.S. 715, 726 (1966) ("It has consistently been recognized that pendent jurisdiction is a doctrine of

[5] At oral argument on May 8, 2014, NetApp's counsel conceded that NetApp does not know whether any of the six individual Defendants other than Weber and Binning have any knowledge of each other, further indicating that NetApp has not fully investigated the factual basis for alleging an overarching scheme.

discretion, not of plaintiff's right."). The factors of economy, convenience, fairness, and comity further confirm that NetApp's remaining state law claims should be dismissed. This case is still at the pleading stage, and no formal discovery has taken place. *See* ECF No. 63 at 21-22. Judicial resources are best conserved by dismissing the case at this stage. The claims against Reynolds and against the employees involve different conduct, legal theories, and geographic locations, and will thus likely require different sources of proof. Furthermore, dismissal promotes comity as it enables California courts to interpret the multiple, overlapping questions of state law that NetApp presents.[6] For these reasons, the Court declines to exercise supplemental jurisdiction over NetApp's claims against Weber, Klute, Glick, Binning, and Alduino.

2. Claims Against Reynolds and Nimble

Nimble alleges multiple state law claims against both Reynolds and Nimble. As explained above regarding the former employee Defendants, claims based on conduct other than Reynolds's illegal computer access are not sufficiently related to the CFAA claims to warrant supplemental jurisdiction. Accordingly, the Court looks to the substance of the remaining claims against Reynolds and Nimble for overlap with the CFAA allegations.

Against Reynolds, NetApp pleads claims for trespass to chattel, breach of contract, and unfair competition. NetApp's assertions for these claims are based on the same conduct alleged for the CFAA claim, namely Reynolds's unauthorized access of NetApp's computer systems. *See, e.g.*, First Am. Compl. ¶ 113 (breach of contract; "Reynolds breached the Use Restrictions by engaging in the unauthorized reproduction and/or distribution of the Synergy software program, data, and portions thereof."). Accordingly, they form a common nucleus of operative facts with the CFAA allegations. The state law claims do not predominate because the underlying conduct is the same and will likely involve similar sources of proof. Therefore, the Court elects to retain supplemental jurisdiction over the state law claims against Reynolds.

Against Nimble, NetApp pleads claims for trespass to chattel, trade secret misappropriation, intentional interference with contract and contractual relations, and unfair competition. The

[6] NetApp has not provided any reasons why it could not pursue all of its causes of action in California state court.

misappropriation and intentional interference claims depend solely on the former employees' theft of proprietary information, not on Reynolds's alleged CFAA violations. *See* First Am. Compl. ¶¶ 102-04 ("Nimble acquired NetApp trade secret information from Weber and Klute . . . ."); 157-59 ("Nimble interfered with the contracts" of the employees). Therefore, the Court declines to exercise jurisdiction over these claims against Nimble.

NetApp's unfair competition cause of action against Nimble is based on Nimble's "unlawful" conduct with regard to the CFAA, *id.* ¶ 167, and on Nimble's "'unfair' business practices" regarding NetApp's former employees and confidential information, *id.* ¶¶ 168-69. As explained above, NetApp's CFAA claim against Nimble is dismissed with leave to amend. Thus, the Court dismisses with leave to amend NetApp's unfair competition cause of action based on Nimble's alleged unlawful conduct with regard to the CFAA. The Court need not reach Nimble's other arguments for dismissal under Rule 12(b)(6) or for a more definite statement under Rule 12(e). Similarly, NetApp's trespass to chattel claim against Nimble is based on Nimble's alleged unlawful conduct with regard to the CFAA, *see id.* ¶¶ 93-95, and the Court dismisses this claim with leave to amend. The Court need not reach Nimble's other arguments against this claim.

On the other hand, the Court declines jurisdiction over NetApp's unfair competition cause of action against Nimble for Nimble's alleged unfair business practices for the same reasons that the Court declines supplemental jurisdiction over NetApp's state law claims against NetApp's former employees.

D. Sufficiency of Remaining Claims Against Reynolds

Because the Court denies Reynolds's motion to dismiss NetApp's CFAA claim and exercises supplemental jurisdiction over the remaining state law claims alleged against him, the Court addresses Reynolds's motion to dismiss those claims under Rule 12(b)(6).

1. Trespass to Chattel and Unfair Competition

Reynolds argues that NetApp's causes of action for trespass to chattel and unfair competition (Cal. Bus. & Prof. Code § 17200) are preempted by California's Uniform Trade Secrets Act ("CUTSA"). *See* Reynolds Mot. at 17-18. The Court agrees.

By statute, the CUTSA supersedes other civil remedies based on trade secret misappropriation. *See* Cal. Civ. Code § 3426.7(b)(2) ("This title does not affect . . . other civil remedies that are not based upon misappropriation of a trade secret."). California courts have ruled that "CUTSA's 'comprehensive structure and breadth' suggests a legislative intent to occupy the field," and that CUTSA preempts common law claims that are "'based on the same nucleus of facts as the misappropriation of trade secrets claim for relief.'" *K.C. Multimedia, Inc. v. Bank of Am. Tech. & Operations, Inc.*, 171 Cal. App. 4th 939, 954-58 (2009) (citations omitted).[7] The test for whether a claim overlaps with the CUTSA involves "a factual inquiry, one that examines the conduct alleged in the claim." *Id.* at 958. Under this inquiry, courts have found that CUTSA can preempt claims for unfair competition under § 17200. *Id.* at 961-62 (affirming preemption ruling because "appellant's statutory unfair competition claim rests squarely on its factual allegations of trade secret misappropriation"). Indeed, this Court has dismissed claims including trespass to chattel and unfair competition due to CUTSA preemption. *See Sunpower Corp. v. SolarCity Corp.*, No. 12-CV-00694-LHK, 2012 U.S. Dist. LEXIS 176284, at *38-47 (N.D. Cal. Dec. 11, 2012) (dismissing claims because "each of SunPower's Non-Trade Secret Claims alleges in essence that Defendants violated SunPower's rights by acquiring, disclosing, and/or using, without consent (*i.e.* misappropriating) SunPower's proprietary information.").

Here, NetApp's allegations against Reynolds regarding trespass to chattel and unfair competition stem entirely from misappropriation of proprietary information, and are thus preempted. For trespass to chattel, NetApp alleges its computer systems "are repositories of valuable proprietary information," First Am. Compl. ¶ 93, and the only such value that NetApp identifies is derived from "its exclusivity," NetApp Reynolds Opp'n at 20. Similarly, for unfair competition, NetApp states only that "Reynolds and Nimble's conduct "is 'unlawful' because, among other reasons, they violated the Computer Fraud and Abuse Act and committed trespass to chattels." First Am. Compl. ¶ 167. Therefore, NetApp has not alleged any misconduct by

[7] Federal courts have followed California courts' interpretation of the preemptive effect of the CUTSA. *See Mattel, Inc. v. MGA Entm't, Inc.*, 782 F. Supp. 2d 911, 987 (C.D. Cal. 2010) ("In an effort to align with the California courts that have addressed this issue, the Court concludes that UTSA supersedes claims based on the misappropriation of confidential information, whether or not that information meets the statutory definition of a trade secret.").

Reynolds with respect to these two claims other than theft of secret information. *See Heller v. Cepia, LLC*, No. C 11-01146 JSW, 2012 U.S. Dist. LEXIS 660, at *20 (N.D. Cal. Jan. 4, 2012) (noting that "common law claims premised on the wrongful taking of information that does not qualify as a trade secret are also superseded" by CUTSA).

NetApp does not contest the conclusion that these claims are factually co-extensive with CUTSA. Rather, NetApp argues only that preemption does not apply because NetApp did not plead a CUTSA claim against Reynolds. *See* NetApp Reynolds Opp'n at 19. This argument is meritless. NetApp identifies no authority stating that preemption applies only if a CUTSA claim is actually pleaded; indeed, such a rule would defeat preemption by allowing plaintiffs to intentionally omit CUTSA claims in favor of other claims. Moreover, courts have held that "CUTSA provides *the exclusive civil remedy* for conduct falling within its terms." *Silvaco Data Sys. v. Intel Corp.*, 184 Cal. App. 4th 210, 236 (2010) (emphasis added), *overruled on other grounds by Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310 (2011). *See also Kovesdy v. Kovesdy*, No: C 10-02012, 2010 U.S. Dist. LEXIS 100940, at *8 (N.D. Cal. Sept. 13, 2010) ("The UTSA provides the exclusive remedy for trade secret misappropriation under California law." (citing *Silvaco*)); *Mattel*, 782 F. Supp. 2d at 961 ("An allegation of trade secret misappropriation is not a prerequisite to UTSA supersession."). Accordingly, NetApp's claims for trespass to chattel and unfair competition against Reynolds are dismissed with leave to amend. While it appears unlikely that NetApp can allege facts that would avoid preemption of these claims against Reynolds, it is not evident that amendment is currently futile.[8] *See* Reynolds Mot. at 18-19.

2. Breach of Contract

Reynolds further moves to dismiss NetApp's claim for breach of contract, arguing that NetApp "has failed to plausibly allege Reynolds's breach or any damages." Reynolds Mot. at 19-20. The Court disagrees. NetApp stated that Reynolds agreed to certain contractual restrictions for use of NetApp's Synergy software and breached those restrictions through "unauthorized reproduction and/or distribution of the Synergy software program, data, and portions thereof," and

[8] The Court need not address Reynolds's separate arguments for dismissing the claim for trespass to chattel. The Court also need not reach the parties' arguments regarding CUTSA preemption of other causes of action against other defendants at this time.

by "use[] of the confidential and proprietary information contained therein." First Am. Compl. ¶¶ 112-13. Reynolds argues that the First Amended Complaint is "bereft of any factual allegations that Reynolds engaged in any such activities." Reynolds Mot. at 19. However, NetApp alleged that Reynolds accessed Synergy six times in June 2013 and obtained confidential information without authorization, in violation of a Download Warning. First Am. Compl. ¶¶ 49, 51. Additionally, NetApp has alleged that Reynolds's improper access caused competitive harm by disseminating confidential information. *See id.* ¶¶ 53-54, 114-15. Accordingly, NetApp has adequately alleged breach of contract against Reynolds.

IV. CONCLUSION

For the foregoing reasons, Defendants' motions to dismiss are GRANTED IN PART AND DENIED IN PART as follows.

Reynolds's motion to dismiss for lack of personal jurisdiction is denied. Reynolds's motion to dismiss NetApp's CFAA claim with respect to § 1030(a)(5) is granted with leave to amend, and otherwise denied. Reynolds's motion to dismiss NetApp's claims for trespass to chattel and unfair competition are granted with leave to amend. Reynolds's motion to dismiss NetApp's claim for breach of contract is denied.

Nimble's motion to dismiss NetApp's CFAA claim is granted as to all pleaded CFAA provisions with leave to amend. Nimble's motion to dismiss NetApp's claims for trespass to chattel and for unfair competition (as to the allegations regarding "unlawful" conduct with regard to the CFAA) is granted with leave to amend. The Court declines supplemental jurisdiction over NetApp's state law claims against Nimble for trade secret misappropriation, intentional interference with contract and contractual relations, and unfair competition (as to the allegations regarding "'unfair' business practices").

The employees' motion to dismiss all of NetApp's claims for lack of supplemental jurisdiction is granted.

NetApp's Request for Judicial Notice is granted. NetApp's motion for leave to conduct jurisdictional discovery is denied as moot.

Defendants' prior motions to dismiss (ECF Nos. 22-24) and NetApp's prior motion for leave to conduct jurisdictional discovery (ECF No. 26), which were withdrawn without prejudice by stipulation before NetApp's First Amended Complaint, are denied as moot.

If NetApp fails to file an amended complaint within 21 days of this Order or to cure the deficiencies addressed in this Order, these claims will be dismissed with prejudice. Plaintiff may not add new claims or parties without leave of the Court or stipulation by the parties pursuant to Federal Rule of Civil Procedure 15.

IT IS SO ORDERED.

Dated: May 12, 2014

Lucy H. Koh

LUCY H. KOH
United States District Judge